Review Article

International Journal of Advanced Computer Research, Vol 10(47)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2019.940152

A survey of biometric approaches of authentication

Nuhu Yusuf*, Kamalu Abdullahi Marafa, Kamila Ladan Shehu, Hussaini Mamman and Mustapha Maidawa
Lecturer, Department of Management and Information Technology, Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria

Received: 20-December-2019; Revised: 19-March-2020; Accepted: 22-March-2020

Abstract
The increasing need for better authentication methods against hackers has called for the use of the biometric authentication method to guard against unauthorized access into the systems. The used of human characteristics for biometrics provides authentication for different kind of systems. However, poor quality of authentication still allows hackers gaining access to these systems. Many biometrics authentication approaches have been proposed to improve the authentication accuracy and other related quality measures. This survey aims to provide a state-of-the-art fingerprint and password biometric authentication approaches. Their challenges have been presented and discussed in terms of biometric authentication. Furthermore, the strengths and weaknesses of each of the fingerprint and password biometric authentication are discussed and compared. The findings show that fingerprint image quality and password authentication is still an active research area where performance requires improvement. Also, the graphical password indicates a promising future direction for enhancing password methods.

Keywords
Biometrics, Authentication, Fingerprint, Password, Information security.

1.Introduction
Information security refers to a means of preventing unauthorized users from access to information. Risk management usually adopts in information security to provide solutions to security challenges by minimizing risks. Risk can be minimized by administrative control and defense mechanisms. Access control can also enforce the user right access and thereby minimizing risks. Authentication is one of the techniques used in access control systems to protect unauthorized access. Many approaches for authentication have been proposed to address security challenges. These approaches have a conflict with the system usability and therefore required the modification of tradition password techniques for better solutions. Information Authentication is the common method used by security experts to verify the users' identities before getting access right into the system. Access controls are enforced for all users, irrespective of categories they belong. Traditional authentication methods [1] were enough to protect the unauthorized access right as many security breaches were reported. Therefore, advanced security methods that are based on human features required.

Biometrics are a strong authentication method based on certain human characteristics. These human characteristics are distinct to each individual and the selection of each requires careful assessment of its benefits and shortcomings. Different biometric methods exist, ranging from simple passwords, fingerprint and palm print and to more complex ones such as DNA. The fingerprint is one of the biometrics methods that are impossible for unauthorized users to alter because it utilizes friction ridges of the finger. Palm prints required an image of the hand, palm region to compare palms for giving access right. As the most common method, people prepared using a password to secure their system rather than using complex algorithms.

Biometric methods prove their capability of preventing unauthorized user access. However, large-scale review required on some of the methods to be able to understand recently added contributions. The previous contribution on this is given by Padma and Srinivasan [2] which focused on the biometric authentication review in cloud computing. Prasad et al. [3] present fingerprint biometric authentication methods where they review various fingerprint recognition system and their application. However,

*Author for correspondence

there is needed to look into other biometric methods as the paper only considers the fingerprint method. This paper presents a survey of biometric authentication methods, specifically compared fingerprint and password methods as the most commonly used by people.

2.Literature review

Biometric authentication attracts the attention of both researchers and practitioners and it's now replacing other authentication methods such as passwords. This is because user behaviour patterns can be easily used for identification. These human characteristics cannot be easily stolen or forgot and can useful for authentications. For instance, face, fingerprint, iris and voice could easily identify users during authentication and unauthorized users would not get access. Tekade and Shende [4] believe that biometric technology is capable of solving personal identity security issues for many critical application areas. Parkavi et al. [5] present the importance of biometrics in using multiple personal identification techniques for authenticating users. Kakkad et al. [6] present the importance of user authentication techniques to authenticate images on clouds.

The biometric authentication was introduced to identified and control access to a system [4]. Biometrics can be human characteristics, for instance, fingerprint, face recognition, iris recognition, retina and palm print [5]. Through biometric recognition, users' identities are verified based on some certain measurements. To provide proper authentication, the biometric authentication usually utilizes fingerprint, eye scanners, facial recognition, hand geometry and passwords authentication approaches. The fingerprint approach operates based on fingerprint scanners such as optical, capacitive and ultrasound [7]. The optical takes the finger photo, identify patterns and compile into codes for proper security identification. Eye scanner approach provides authentication based on retina and iris scanner. The retina and iris remain with a person throughout their life and as such can be easily accessible. The retina scan uses light to illuminate eye blood vessels. The idea for this is that people have different retina tissues in blood vessels. Iris scanner uses a photo of individuals and uses for authentication. Facial recognition approach can be either extracting person face image or using skin texture analysis for authentication. Hand geometry approach uses palm thickness for biometric authentication. Though, the low accuracy [6] serves as the drawback to this approach. Biometric authentication provides authentication security process to verify user identity [4]. The biometric authentication has been characterized as ease of use method. This is because users can use it at any time they required to use. The biometric authentication also makes difficult for hackers to discover any weakness and have access to the system [8]. However, a certain limitation exists for biometric authentication such used by proxy and remote recovery. To use biometric authentication, the actual person involve d must be physically present and other people cannot authenticate on behalf of others. Additionally, some of the authentication methods do have recovery methods but there is absent of such recovery for biometric authentication. *Figure 1* presents some of the common biometric authentication methods.

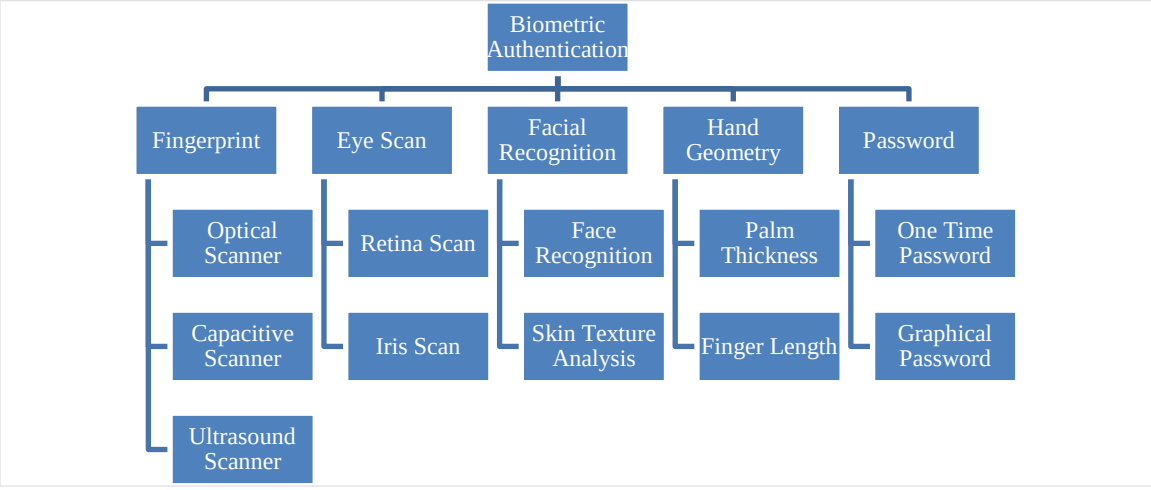

Figure 1 Biometric authentication methods

3.Methods

The most often used biometric authentication approaches in either simple or complex systems are fingerprint and passwords methods.

3.1Fingerprint biometric authentication

The fingerprint is an important mechanism for detecting crime and prevents unauthorized access to the system. Erika Rahmawati et al. [9] believe fingerprint technology can be used with a digital signature to improve the security of mobile applications, specifically when sending and receiving documents. Furthermore, Kamelia et al. [10] examine the significant of fingerprint method in taking online attendance using mobile phones. They provide the possibility of integrating fingerprint with GPS via Arduino and achieved 1.39 seconds average response time. Goicoechea-Telleria et al. [11] investigate how fingerprint adoption in smartphones becomes a worry some due to sensor issues. Hwang et al. [12] provide a template for achieving higher accuracy in fingerprint recognition for mobile devices. You and Wang [13] proposed a fingerprint method that is based on a fuzzy vault scheme. Wireless devices require fingerprint for data security as such, Lin et al. [14] suggest dimensional reduction that utilizes machine learning algorithms as an authentication solution. Dimensional reductions provide effective decisions on data reduction. In addition to that, Ma et al.[15] presents a multi-dimension algorithm to provide cellular network security. However, Sadhukhan et al. [16] analyses the performance of clustering based fingerprint for smartphones devices.

Engelsma et al. [17] suggested how fingerprint can be enhancing in future to avoid image variation results from fingerprint captures. They presented a universal 3d fingerprint target as an alternative to improve images variations. Similarly, fingerprint higher resolution in terms of 3d can also be achieved using sweat gland extraction [18] which utilizes cells positions. However, Valdes-Ramirez et al. [19] reviewed fingerprint features for identifying latent fingerprint based on minutiae. Makhija et al. [20] analysed the performance of various latent fingerprint techniques which required further improvements.

3.2Password biometric authentication

Password authentication is the process of verifying the access right of the user through the use of a password. User may be allowed to set up a simple password using text. But these simple texts are subjects to attacks. Maqbali and Mitchell [21] suggested the generating of password automatically without users involvements. This will be in line with international standard practise for password requirements authentication.

The purpose of password authentication is to make authorize users to kept secret access right so that unauthorized would not get access to. The passwords should not be easy for password attacks to guess. Password attackers can easily gain access to weak passwords. Rahiemy et al. [22] present that the lack of password complexity serves as the source for attackers. In addition to that, Tabrez and Sai [23] also believe that weak passwords always motivate attackers. Zhang et al. [24] argued that a technique can design in such a way that user may constantly change the password before attackers have access. The technique only takes into consideration the dictionary attacks while forgetting that other attacks may provide serious damages than dictionary attacks. Password attacks are various techniques used to gain access to the password by either guessing or stealing. It could be dictionary attacks where people's names, date of births, or lower/uppercase letters would be trying and retry till getting the actual password. *Figure 1* presents how dictionary attacks work. Erdem and Sandıkkaya [25] support the use of the one-time password and they proposed a technique based on OTP where cloud provider would be located as the cloud as service and then analyze the user before given access. Default password may be discovered by either Trojan horse or backdoors via network trafficking. Intruders also used social engineering to have access to the passwords via emails or any other alternative methods. Bruteforce attacks are other attacks based on trial and error to get access to the password.

Mohamedali and Fadlalla [26] present different categories of password attacks and stated the benefits and shortcomings of each attack. They suggest more friendly methods to address these attacks without complicating with usability. These attacks include among others the Phishing, Man-in-the-Middle, etc. Zheng and Jia [27] suggest the use of separators between keystrokes to address the leaked password issues. This means that the blank space is inserted within the password for better authentications. If the passport with spaces corresponds with the users' inputs, then access right will be granted. However, Hwang et al. [28] proposed the use of Smart Card as an authentication method instead of a general password. They try to address password guessing attacks using complex smart card implementations.

4.Results

This section presents the results of the two major biometric authentications taking into consideration their strengths and limitations.

4.1Results of fingerprint biometric authentication approach

Table 1 present the comparison of various fingerprint techniques. Wu and Chiu [29] present solutions to poor fingerprint quality to ensure better fingerprint recognition for authentication. Their work used ridge features techniques which different individuals and achieved almost 99% accuracy. In addition to that, Tang et al. [30] examine how Hessian matrix and short-time Fourier transform (STFT) would improve fingerprint images quality utilizes fingerprint textures. The result indicates 0.799 second processing time has been reduced. Furthermore, Liban and Hilles [31] suggest enhancing latent fingerprint to improve fingerprint quality so that reasonable processing time would be achieved. However, Koptyra and Ogiela [32] argued that higher fingerprint processing time will be achieved if enhancing Histograms of Oriented Gradients (HOG) technique.

Patel et al. [33] enhanced O' Gorman filter to address minutiae points' extraction problem. The result achieved mean square error (MSE) and peak signal to noise ratio (PSNR) of 6% and 39% respectively. Similarly, Sudiro et al. [34] used Artificial Neural Network to address Fingerprint extraction issues while achieving 41% False Acceptance Rate. Kim et al. [35] also used a deep neural network to address issues arising from fingerprint collections. Cao and Jain [36] present fingerprint synthesis technique to reduce processing time error of fetching fingerprint images from the database. Nuraisha and Shidik [37] stated that fake fingerprints cause longer processing time and as such normalization is required to get higher accuracy results. Han et al. [38] improve fingerprint image impulse noise using Adaptive Median Filter.

4.2Results of password biometric authentication approach

With all the security challenges of traditional password, Taufiq and Ogi [39] suggest improvement of existing passwords techniques to strengthen security rather than adopting other complex methods. They present a method that utilizes one-time password known as Raspberry Pi at the access control level. Though it is difficult for attackers to repay attacks on password because the new password will be assigned, the network response time will force another challenge. Furthermore, Zaki et al. [40] believe that text passwords can be enhanced using different pattern keys ranging from simple to complex ones. However, Lekshmi et al. [41] suggested the neural network approach as an alternative password method, especially if integrated with fuzzy rules. Bhola et al [42] examine how android device will be used to improve on password methods. Scaria and Megalingam [43] present a complex method that incorporates OTP, biometrics and noisy passwords.

Graphical passwords have been successfully implemented to overcome text-based passwords challenges but still required more improvements. Bilgi and Tugrul [44] integrated images in a password method to provide access right. Their approach provides more benefits compared to ordinary text-based passwords but does not clearly state how shoulder surfing attacks would be minimized. Moreover, Fayyadh et al. [45] present a graphical method that allows the user to create shapes during their registration and thereby required to draw such shapes when accessing the system. Their approach is quite an improvement compared to Bilgi and Tugrul [44]. Zhang et al [46] approach is difficult to implement and can be conflicting with usability. Table 2 shows the evaluation of password biometric authentication approaches.

Table 1 Evaluation of Fingerprint Biometric Authentication Approaches

Authors	Problem	Techniques	Metrics/results	Benefits	Limitations
Wu and Chiu (2017) [29]	poor fingerprint quality	Ridge Features	Accuracy of 99.00%, and 99.09%	Successfully classified ridges features	Not suitable for large datasets
Patel et al. (2017) [33]	minutiae points extraction	Enhanced O'Gorman Filter	MSE = 6.698 PSNR = 39.871	Better results on O'Gorman compare to Gabor	Doesn't show overall fingerprint performance
Cao and Jain (2018) [36]	fingerprint images database	Fingerprint Synthesis	Time: 512 × 512 in 12 muinute	Provide a better quality image	Doesn't incorporating diversity criteria in the training process

Authors	Problem	Techniques	Metrics/results	Benefits	Limitations
Abdilahi Liban and Hilles (2018) [47]	Fingerprint images quality	Enhanced Latent fingerprint	RMSE = 0.023199 PSNR = 81.07826	improved matching accuracy	latent fingerprint images still overlapped
Safira Nuraisha et al (2018) [37]	fake fingerprints	Normalization	Accuracy of 24%	Increased accuracy of detecting fake fingerprint images	Inefficient features extraction
Szymkowski and Saeed (2018) [48]	Fingerprint recognition	Sectorization	Accuracy of 100%	Provide a new way to reach a satisfactory level of identification accuracy	Changes in changes in their fingerprint patterns may still present
Han et al. (2018) [38]	filtering window size noise	Adaptive Median Filter	PSNR = 44	Present feasible for fingerprint image enhancement	impulse noise still present
Kim et al. (2019) [35]	Collecting fingerprints	deep neural networks	average detection error rate=1.57%	Generate real fingerprint with certain characteristics	Time-consuming
Sudiro et al. (2017) [34]	Fingerprint extraction	simple minutiae point extraction	FAR= 41.57% FRR= 41.13%, EER= 41.35%	minutiae extraction improvement	still lack accuracy due to the high value of FAR
Tang et al. (2017) [30]	Fingerprint Image quality	Hessian matrix and short-time Fourier transform (STFT)	Processing time = 0.799 s	increased the contrast greatly according to the structural characteristics	low contrast between ridge still need improvement

Table 2 Evaluation of password biometric authentication approaches

Authors	Problem	Techniques	Benefits	Limitations
Taufiq and Ogi (2018) [39]	password leakage attacks	Raspberry Pi	Improve one-time password mutual authentication	Run with RSA
Zaki et al. (2018) [40]	password authentication	combination of pattern, key, and dummy digits	minimizes different password attacks and usability issues	Expensive to implement
Lekshmi et al. (2018) [41]	password authentication	Hopfield Neural Network with fuzzy logic	provides better accuracy and response time	Not easier compare to graphical passwords
Bhola et al. (2017) [42]	Cybercrimes	Android Device and One-Way Function	Improved dynamic password Authentication	Cannot handle multiple websites authentication
Bilgi and Tugrul (2018) [44]	password authentication	Shoulder-Surfing Resistant Graphical passwords	faster and easier authentication processes	shoulder surfing problem
Mehrube and Nguyen (2018) [49]	password authentication	Real-time Eye Tracking	The smart camera can capture and store PIN	incorporating the PIN identification algorithm into the-real-time
Othman et al. (2018) [50]	password authentication	Graphical Authentication with Shoulder Surfing Resistant	demonstrate the robustness, security strength and the functionality	A higher number of direction authentication exposure
Fayyadh et al (2018) [45]	password authentication	graphical password (2D Shapes)	effective against the brute force attacks, the dictionary attacks, and the keylogger attacks	Difficult to remember the number of used shapes when larger
Sudramurthy et al (2017) [51]	password authentication	Honey Password	Pointed out the strength of the honey word system depends on the AES Algorithm	Limited to online purchase

5.Discussion

In section 3, the biometric authentication methods are presented to provide proper authentication. The fingerprint authentication accuracy and PSNR have been observed with different levels of performance. Reasonable results have been obtained for accuracy which indicates how accurate some of these techniques have in addressing fingerprint challenges. The PSNR results indicate additional improvement is required. Moreover, the techniques used are mostly

enhancement of the existing techniques for fingerprint and their limitations was highlighted. Additionally, the techniques appear to solve certain problems, especially for poor quality recognition. For instance, ridges feature technique successfully classified and improved poor quality of the fingerprint. Despite the quality of this technique in recognizing fingerprint, the ridges feature technique not suitable for large datasets. This is because of difficulties in counting the number of fingerprint ridges. O'Gorman filter technique has also limitation in showing fingerprint performance when compared to other methods such as Gabor in extracting minutiae points. The fingerprint synthesis doesn't take diversity into account when addressing the fingerprint image database. The latent fingerprint and sectorization techniques improved accuracy, but the image still overlapped while minimization contains low accuracy results. This is because fake fingerprint may be difficult to detect if complex mechanisms have not put in place for detection. A deep neural network is time-consuming in collecting fingerprints. The STFT technique also provides efficient, timely results due to contrast increased. Moreover, impulse noise is still present in the adaptive media filter technique. In password, biometric authentication methods, graphical password techniques have some issues regarding the remembering of a various number of shapes which may lead to poor authentication. Though, the graphical passwords techniques provide an effective measure against hackers. Using Hopfield neural network with fuzzy logic can possibly eliminate this problem. The Hopfield neural network with fuzzy logic can provide better accuracy for authentication compared with some of the graphical password's techniques. Pattern key and dummy digits are expensive to implement compared with Raspberry Pi based on the one-time password. Real-time eye-tracking techniques can be a good technique for authentication compared with smart camera capture with store PIN which is easily altered.

6.Conclusion and future work

Biometric authentication is identification and verification, which consider human characteristics to improve system security. The aim is to identify and authenticate access to any component of the system. There are many biometric authentication methods currently available. This work only considers the two most widely used methods which are the fingerprint and passwords methods. Various proposed fingerprint techniques show much improvement in achieving high image quality. However, the fingerprint image quality still required improvement to recognize fingerprint. Moreover, the password method comprises text and graphical passwords. Graphical password authenticates users based on the grid selection algorithm. The algorithm can prevent not only shoulder surfing attacks, but also other related password attacks. Besides that, we highlighted some features of various biometric authentication techniques. Additionally, we discussed some of the strengths and challenges of biometric authentication. In general, both fingerprint and password methods have proved effective for biometric authentication. However, regarding future work, all simple and complex biometric authentication methods should be considered for a better understanding.

Acknowledgment

We wish to thank the Department of Management & Information Technology ATBU Bauchi, Faculty of Management Science ATBU Bauchi as well as the Management of Abubakar Tafawa Balewa University Bauchi for their support and encouragement.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Bharathi S, Sudhakar R. Biometric recognition using finger and palm vein images. Soft Computing. 2019; 23:1843-55.

[2] Padma P, Srinivasan S. A survey on biometric based authentication in cloud computing. In international conference on inventive computation technologies 2016 (pp. 1-5). IEEE.

[3] Prasad PS, Devi BS, Reddy MJ, Gunjan VK. A survey of fingerprint recognition systems and their applications. In international conference on communications and cyber physical engineering 2018 (pp. 513-20). Springer, Singapore.

[4] Tekade P, Shende P. Enhancement of security through fused multimodal biometric system. In international conference on computing, communication, control and automation 2017 (pp. 1-5). IEEE.

[5] Parkavi R, Babu KC, Kumar JA. Multimodal biometrics for user authentication. In 11th international conference on intelligent systems and control 2017 (pp. 501-5). IEEE.

[6] Kakkad V, Patel M, Shah M. Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design. 2019; 2:233-48.

[7] Nakanishi I, Maruoka T. Biometric authentication using evoked potentials stimulated by personal ultrasound. In international conference on telecommunications and signal processing (TSP) 2019 (pp. 365-8). IEEE.

[8] Vittori P. Ultimate password: is voice the best biometric to beat hackers?. Biometric Technology Today. 2019; 2019(9):8-10.
[9] Rahmawati E, Listyasari M, Aziz AS, Sukaridhoto S, Damastuti FA, Bachtiar MM, et al. Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In international electronics symposium on engineering technology and applications (IES-ETA) 2017 (pp. 234-8). IEEE.
[10] Kamelia L, Hamidi EA, Darmalaksana W, Nugraha A. Real-time online attendance system based on fingerprint and GPS in the smartphone. In international conference on wireless and telematics 2018 (pp. 1-4). IEEE.
[11] Goicoechea-Telleria I, Garcia-Peral A, Husseis A, Sanchez-Reillo R. Presentation attack detection evaluation on mobile devices: simplest approach for capturing and lifting a latent fingerprint. In international carnahan conference on security technology 2018 (pp. 1-5). IEEE.
[12] Hwang D, Lee H, Bae G, Son S, Kim J. Fingerprint template management for higher accuracy in user authentication. In international conference on electronics, information, and communication 2018 (pp. 1-4). IEEE.
[13] You L, Wang T. A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion. Soft Computing. 2019; 23(11):3843-51.
[14] Lin Y, Zhu X, Zheng Z, Dou Z, Zhou R. The individual identification method of wireless device based on dimensionality reduction and machine learning. The Journal of Supercomputing. 2019; 75:3010-27.
[15] Ma L, Jin N, Zhang Y, Xu Y. RSRP difference elimination and motion state classification for fingerprint-based cellular network positioning system. Telecommunication Systems. 2019; 71:191-203.
[16] Sadhukhan P. Performance analysis of clustering-based fingerprinting localization systems. Wireless Networks. 2019; 25:2497-510.
[17] Engelsma JJ, Arora SS, Jain AK, Paulter NG. Universal 3D wearable fingerprint targets: advancing fingerprint reader evaluations. IEEE Transactions on Information Forensics and Security. 2018; 13(6):1564-78.
[18] Sun S, Guo Z. Sweat glands extraction in optical coherence tomography fingerprints. In international conference on security, pattern analysis, and cybernetics 2017 (pp. 579-84). IEEE.
[19] Valdes-Ramirez D, Medina-Pérez MA, Monroy R, Loyola-González O, Rodríguez J, Morales A, et al. A review of fingerprint feature representations and their applications for latent fingerprint identification: trends and evaluation. IEEE Access. 2019; 7:48484-99.
[20] Makhija S, Khatwani A, Roja MM. Performance analysis of latent fingerprint enhancement techniques. In international conference on innovative mechanisms for industry applications 2017 (pp. 96-100). IEEE.
[21] Al Maqbali F, Mitchell CJ. AutoPass: an automatic password generator. In international carnahan conference on security technology 2017 (pp. 1-6). IEEE.
[22] Rahiemy MZ, Sukarno P, Jadied EM. Hardening the virtual password authentication scheme. In international conference on information and communication technology 2018 (pp. 429-34). IEEE.
[23] Tabrez S, Sai DJ. Pass-Matrix authentication a solution to shoulder surfing attacks with the assistance of graphical password authentication system. In international conference on intelligent computing and control systems 2017 (pp. 776-81). IEEE.
[24] Zhang S, Zeng J, Zhang Z. Password guessing time based on guessing entropy and long-tailed password distribution in the large-scale password dataset. In international conference on anti-counterfeiting, security, and identification 2017 (pp. 6-10). IEEE.
[25] Erdem E, Sandıkkaya MT. OTPaaS—one time password as a service. IEEE Transactions on Information Forensics and Security. 2018; 14(3):743-56.
[26] Mohamedali IA, Fadlalla Y. Securing password in static password-based authentication: a review. In sudan conference on computer science and information technology 2017 (pp. 1-5). IEEE.
[27] Zheng W, Jia C. CombinedPWD: a new password authentication mechanism using separators between keystrokes. In international conference on computational intelligence and security 2017 (pp. 557-60). IEEE.
[28] Hwang MS, Cahyadi EF, Chou YC, Yang CY. Cryptanalysis of kumar's remote user authentication scheme with smart card. In international conference on computational intelligence and security 2018 (pp. 416-20). IEEE.
[29] Wu CJ, Chiu CT. Dry fingerprint detection for multiple image resolutions using ridge features. In international workshop on signal processing systems 2017 (pp. 1-5). IEEE.
[30] Tang Y, Jiang L, Hou Y, Wang R. Contactless fingerprint image enhancement algorithm based on hessian matrix and STFT. In international conference on multimedia and image processing 2017 (pp. 156-60). IEEE.
[31] Liban A, Hilles SM. Latent fingerprint enhancement based on directional total variation model with lost minutiae reconstruction. In international conference on smart computing and electronic enterprise 2018 (pp. 1-5). IEEE.
[32] Koptyra K, Ogiela MR. Multiply information coding and hiding using fuzzy vault. Soft Computing. 2019; 23:4357-66.
[33] Patel MB, Patel RB, Parikh SM, Patel AR. An improved O'Gorman filter for fingerprint image enhancement. In international conference on energy, communication, data analytics and soft computing 2017 (pp. 200-9). IEEE.
[34] Sudiro SA, Wardhani IP, Wardijono BA, Handias B. Fingerprint matching application using hardware based artificial neural network with matlab. In 5th

international conference on electrical, electronics and information engineering 2017 (pp. 66-70). IEEE.
[35] Kim H, Cui X, Kim MG, Nguyen TH. Fingerprint generation and presentation attack detection using deep neural networks. In conference on multimedia information processing and retrieval 2019 (pp. 375-8). IEEE.
[36] Cao K, Jain A. Fingerprint synthesis: Evaluating fingerprint search at scale. In international conference on biometrics 2018 (pp. 31-8). IEEE.
[37] Nuraisha S, Shidik GF. Evaluation of normalization in fake fingerprint detection with heterogeneous sensor. In international seminar on application for technology of information and communication 2018 (pp. 83-6). IEEE.
[38] Han K, Wang Z, Chen Z. Fingerprint image enhancement method based on adaptive median filter. In 24th Asia-Pacific conference on communications 2018 (pp. 40-4). IEEE.
[39] Taufiq M, Ogi D. Implementing one-time password mutual authentication scheme on sharing renewed finite random sub-passwords using raspberry pi as a room access control to prevent replay attack. In international conference on electrical engineering and informatics 2018 (pp. 13-8). IEEE.
[40] Zaki MH, Husain A, Umar MS, Khan MH. Secure pattern-key based password authentication scheme. In international conference on multimedia, signal processing and communication technologies 2017 (pp. 171-4). IEEE.
[41] Lekshmi K, Krishnaveni KS, Aparna VK. A hopfield neural network approach for authentication of password based on fuzzy logic. In international conference on advances in computing, communications and informatics 2018 (pp. 2471-4). IEEE.
[42] Bhola G, Kaur D, Raj M. Dynamic password authentication protocol using android device and one-way function. In international conference on wireless communications, signal processing and networking 2017 (pp. 1863-6). IEEE.
[43] Scaria BA, Megalingam RK. Enhanced e-commerce application security using three-factor authentication. In second international conference on intelligent computing and control systems 2018 (pp. 1588-91). IEEE.
[44] Bilgi B, Tugrul B. A shoulder-surfing resistant graphical authentication method. In international conference on artificial intelligence and data processing 2018 (pp. 1-4). IEEE.
[45] Fayyadh BE, Mansour K, Mahmoud KW. A new password authentication mechanism using 2D shapes. In international conference on computer science and information technology 2018 (pp. 113-8). IEEE.
[46] Zhang X, Sun H, Yao B, Liu X. A technique based on the module-K super graceful labelling for designing new-type graphical passwords. In advanced information management, communicates, electronic and automation control conference 2018 (pp. 1495-9). IEEE.
[47] Liban A, Hilles SM. Latent fingerprint enhancement based on directional total variation model with lost minutiae reconstruction. In international conference on smart computing and electronic enterprise 2018 (pp. 1-5). IEEE.
[48] Szymkowski M, Saeed K. A novel approach to fingerprint identification using method of sectorization. In international conference on biometrics and kansei engineering 2017 (pp. 55-9). IEEE.
[49] Mehrubeoglu M, Nguyen V. Real-time eye tracking for password authentication. In international conference on consumer electronics 2018 (pp. 1-4). IEEE.
[50] Othman NA, Rahman MA, Sani AS, Ali FH. Directional based graphical authentication method with shoulder surfing resistant. In conference on systems, process and control 2018 (pp. 198-202). IEEE.
[51] Sudramurthy B, Al Obaidy M, Maata RL. Analysis of authentication on online purchase using honey password. In international conference on computational intelligence and computing research 2017 (pp. 1-3). IEEE.

Nuhu Yusuf is a Lecturer in the Management and Information Technology Department at Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. He is currently pursuing his Ph.D. in Information Technology. His current research areas are Data Science, Big data, Data mining, Information Security, Human Computer Interaction and Artificial Intelligence.
Email: ynuhu@atbu.edu.ng

Kamalu Abdullahi Marafa is a Lecturer in the Management and Information Technology Department at Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. He received his Master of Science in Management Information Technology in 2020. His current research areas are Cloud Computing, Information System, Information Security and Human Computer Interaction.
Email: kamarafa@atbu.edu.ng

Kamila Ladan Shehu is a Lecturer in the Management and Information Technology Department at Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. She is currently pursuing her Ph.D. in Management Information Technology. Her current research areas are Electronic Business, Technology Management, Information Security and Human Computer Interaction.
Email: klshehu@atbu.edu.ng

Hussaini Mamman is a Lecturer in the Management and Information Technology Department at Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. He received his Master of Science in Management Information Technology 2019. His current research areas are Data Science, Big data, Data mining, Information Security, Cloud Computing and Artificial Intelligence.
Email: mhussaini@atbu.edu.ng

Mustapha Maidawa is a Lecturer in the Management and Information Technology Department at Abubakar Tafawa Balewa University (ATBU) Bauchi, Nigeria. He is currently pursuing his Ph.D. in Management Information Technology. His current research areas are Cloud Computing, Database Management and Information Security.
Email: mmaidawa@atbu.edu.ng